III. REMARKS

Claims 1-20 are pending in this application. By this amendment, claims 1, 9, 17, 19 and 20 have been amended. These amendments are being made to facilitate early allowance of the presently claimed subject matter. Applicants do not acquiesce in the correctness of the rejections and reserve the right to present specific arguments regarding any rejected claims not specifically addressed. Further, Applicants reserve the right to pursue the full scope of the subject matter of the original claims in a subsequent patent application that claims priority to the instant application. Reconsideration in view of the following remarks is respectfully requested.

Entry of this Amendment is proper under 37 C.F.R. 1.116(b) because the Amendment: (a) places the application in condition for allowance as discussed below; (b) does not raise any new issues requiring further search and/or consideration; and (c) places the application in better form for appeal. Accordingly, Applicants respectfully request entry of this Amendment.

In the Office Action, claims 1-20 are rejected under 35 U.S.C. §101 as allegedly being directed to non-statutory subject matter.

A. SUPPORT FOR INDEPENDENT CLAIMS

The Office has requested the Applicants provide support for the claimed invention. Accordingly, claim 1 provides a computer system for generating a random output stream of bits for encrypting data, the system comprising: an initial evolving state produced from one or more initial keys (see e.g., page 5, lines 4-6; page 15, lines 19-20; FIG. 2, 204; FIG. 7, 706); one or more round functions, each round function being part of a step in a sequence of steps, each step applying the respective round function to a current evolving state to produce a respective new

evolving state for processing by the next step in the sequence, the initial evolving state processed by the first step in the sequence (see e.g., page 5, lines 4-8; page 7, lines 3-7; page 9, lines 1-13; FIG. 3, 304c, 305; FIG. 5, 503, 504); and one or more mask tables produced from one or more of the initial keys, each of the mask tables having one or more masks, one or more of the masks being combined, in each respective step, with the respective new evolving state in a combination operation to create a respective step output, the random output stream being a concatenation of all the respective step outputs (see e.g., page 5, lines 9-13; page 7, lines 7-8; page 8, lines 3-19; FIG. 3, 304a, 307; FIG. 4, 410, 430), and one or more of the masks in the mask tables being replaced by one or more replacement masks after the combination operation is performed a predetermined number of times, (see e.g., page 7, lines 10-14) the replacement masks not being linear combinations of prior masks (see e.g., page 7, line 15-20).

Claim 9 provides a computer system for generating a random output stream of bits for encrypting data, the system comprising: an initial evolving state produced from one or more initial keys (see e.g., page 5, lines 4-6; page 15, lines 19-20; FIG. 2, 204; FIG. 7, 706); one or more round functions, each round function being part of a step in a sequence of steps, each step applying the respective round function to a current evolving state to produce a respective new evolving state for processing by the next step in the sequence, the initial evolving state processed by the first step in the sequence (see e.g., page 5, lines 4-8; page 7, lines 3-7; page 9, lines 1-13; FIG. 3, 304c, 305; FIG. 5, 503, 504); and two or more mask tables produced from one or more of the initial keys, each of the mask tables having one or more masks, one or more of the masks from each table being combined, in each respective step, with the respective new evolving state in a combination of all the respective step outputs (see e.g., page 5, lines 9-13; page 7, lines 7-8;

page 8, lines 3-19; FIG. 3, 304a, 307; FIG. 4, 410, 430).

Claim 17 provides A method for generating a random output stream of bits for encrypting data comprising the steps of: A. producing a current evolving state from one or more initial keys (see e.g., page 5, lines 4-6; page 15, lines 19-20; FIG. 2, 204; FIG. 7, 706); B. producing one or more mask tables from one or more of the initial keys, each of the mask tables having one or more masks (see e.g., page 5, lines 9-13; page 7, lines 7-8; page 8, lines 3-19; FIG. 3, 304a, 307; FIG. 4, 410, 430); C. applying a round function to a current evolving state to produce a respective new evolving state (see e.g., page 5, lines 4-8; page 7, lines 3-7; page 9, lines 1-13; FIG. 3, 304c, 305; FIG. 5, 503, 504); D. replacing the current evolving state with the new evolving state (see e.g., page 7, lines 6-7; FIG. 3, 304b); E. combining one or more of the masks with the current evolving state in a combination operation to create a respective step output (see e.g., page 7, lines 7-8; FIG. 3, 307); F. replacing one or more of the masks in the mask tables by one or more replacement masks after a number of combination operations (see e.g., page 7, lines 10-14), the replacement masks not being linear combinations of prior masks (see e.g., page 7, line 15-20); G. repeating steps C through F one or more times (see e.g., page 7, lines 5-6; FIG. 3); and H. concatenating all the respective step outputs to create the random output stream (see e.g., page 5, lines 12-13).

Claim 19 provides a computer program product having a stored method for generating a random output stream of bits for encrypting data, the method comprising the steps of: A. producing a current evolving state from one or more initial keys (see e.g., page 5, lines 4-6; page 15, lines 19-20; FIG. 2, 204; FIG. 7, 706); B. producing one or more mask tables from one or more of the initial keys, each of the mask tables having one or more masks (see e.g., page 5, lines

9-13; page 7, lines 7-8; page 8, lines 3-19; FIG. 3, 304a, 307; FIG. 4, 410, 430); C. applying a round function to a current evolving state to produce a respective new evolving state (see e.g., page 5, lines 4-8; page 7, lines 3-7; page 9, lines 1-13; FIG. 3, 304c, 305; FIG. 5, 503, 504); D. replacing the current evolving state with the new evolving state (see e.g., page 7, lines 6-7; FIG. 3, 304b); E. combining one or more of the masks with the current evolving state in a combination operation to create a respective step output (see e.g., page 7, lines 7-8; FIG. 3, 307); F. replacing one or more of the masks in the mask tables by one or more replacement masks after a number of combination operations, the replacement masks not being linear combinations of prior masks (see e.g., page 7, lines 10-14); G. repeating steps C through F one or more times (see e.g., page 7, lines 5-6; FIG. 3); and H. concatenating all the respective step outputs to create the random output stream (see e.g., page 5, lines 12-13).

Claim 20 provides a computer system for generating a random output stream of bits for encrypting data, the system comprising: A. means for producing a current evolving state from one or more initial keys (see e.g., page 5, lines 4-6; page 15, lines 19-20; FIG. 2, 204; FIG. 7, 706); B. means for producing one or more mask tables from one or more of the initial keys, each of the mask tables having one or more masks (see e.g., page 5, lines 9-13; page 7, lines 7-8; page 8, lines 3-19; FIG. 3, 304a, 307; FIG. 4, 410, 430); C. means for applying a round function to a current evolving state to produce a respective new evolving state (see e.g., page 5, lines 4-8; page 7, lines 3-7; page 9, lines 1-13; FIG. 3, 304c, 305; FIG. 5, 503, 504); D. means for replacing the current evolving state with the new evolving state (see e.g., page 7, lines 6-7; FIG. 3, 304b); E. means for combining one or more of the masks with the current evolving state in a combination operation to create a respective step output (see e.g., page 7, lines 7-8; FIG. 3, 307); F. means for

replacing one or more of the masks in the mask tables by one or more replacement masks after a number of combination operations, the replacement masks not being linear combinations of prior masks (see e.g., page 7, lines 10-14); G. means for repeating steps C through F one or more times (see e.g., page 7, lines 5-6; FIG. 3); and H. means for concatenating all the respective step outputs to create the random output stream (see e.g., page 5, lines 12-13).

B. REJECTION OF CLAIMS 1-9 UNDER 35 U.S.C. §101

The Office has rejected claims 1-20 for allegedly being directed to non-statutory subject matter. Specifically, the Office states that the invention as claimed does not produce a concrete and tangible result. Applicants have amended claims 1, 9, 17, 19 and 20 to recite, "...generating a random output stream of bits for encrypting data." Claims 2-8, 10-16 and 18 depend from claims 1, 9 and 17, respectively. Applicants assert that this amendment further directs the invention to statutory subject matter by, *inter alia*, more specifically pointing out the concrete and tangible result of data encryption. Accordingly, Applicants request that the rejection be withdrawn.

IV. CONCLUSION

In light of the above, Applicants respectfully submit that all claims are in condition for allowance. Should the Examiner require anything further to place the application in better condition for allowance, the Examiner is invited to contact Applicants' undersigned representative at the number listed below.

Respectfully submitted,

Hunter E. Webb
Reg. No.: 54,593

Date: April 21, 2006

Hoffman, Warnick & D'Alessandro LLC
75 State Street, 14th Floor
Albany, New York 12207
(518) 449-0044
(518) 449-0047 (fax)

RAD/hew